**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

1-27. (Canceled)

28. (Previously presented): The method of claim 30, further comprising the step of:

providing ingress filtering at said logical ports.

29. (Previously presented): The method of claim 30, wherein said security association contains at least two keys, one key for encryption and another key for computing an authentication code, wherein said security association is associated with a VLAN, wherein said authentication code is used to limit traffic at one of said logical ports to members of an entire VLAN, wherein encryption is used to keep traffic private except to members, wherein only stations having said security association belong to said VLAN, and wherein all stations having said security association belong to the same broadcast domain.

30. (Previously presented): The method of claim 31, wherein said access point may serve more than one VLAN by having multiple logical ports associated with it.

31. (Currently amended): In a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for joining a personal virtual local area network (VLAN) served by said access point, comprising steps of:

providing a control channel for authentication of a requester by a creator of said personal VLAN;

using said control channel to relay authentication protocol messages between said creator and said requester;

if said creator can authenticate said requester, then said creator sharing a security association it holds with said requester;

using said security association shared among members of said personal VLAN to identify frames originating from said members, wherein:

if a received frame carries a null virtual LAN ID (VID) or is untagged, then using its source MAC address to determine a preliminary VLAN classification of said received frame; and

if said received frame carries a VID, then using said VID as said preliminary VLAN classification instead;

using said preliminary VLAN classification to index into a table of security associations giving an authentication code key;

said received frame carrying an authentication code computed over a frame payload thereof using a message digest algorithm agreed upon by both said creator and said requester at authentication time and having been recorded in said table of security associations;

a receiver of said received frame re-computing an authentication code, using said authentication code key, over said payload of said received frame;

comparing said re-computed authentication code with said received authentication code;

wherein if said re-computed authentication code and said received authentication code match, then said preliminary VLAN classification becomes a final VLAN classification;

using said final VLAN classification as a value of a VLAN classification parameter of any corresponding data request primitives;

decrypting said received frame using said security association; and

submitting said decrypted frame to a forwarding and learning process;

otherwise, discarding said received frame.

32-37. (Canceled)

38. (Currently amended): A method for segregating traffic among a plurality of end stations associated with a network access point comprising:

an end station from among said plurality of end stations performing an initial authentication operation;

receiving a frame at said end station;

if said received frame carries a null virtual LAN ID (VID) or is untagged, then using its source MAC address to determine a preliminary VLAN classification of said received frame;

if said received frame carries a VID, then using said VID as said preliminary VLAN classification instead;

using said preliminary VLAN classification to index into a table of security associations giving a cryptographic authentication code key;

said received frame including a cryptographic authentication code computed over a frame payload thereof using a cryptographic message digest algorithm that is determined at a time during said initial authentication operation, said cryptographic message digest algorithm being recorded in said table of security associations;

said end station re-computing said cryptographic authentication code, using said cryptographic authentication code key, over said payload of said received frame;

comparing said re-computed cryptographic authentication code with said received cryptographic authentication code;

wherein if said re-computed cryptographic authentication code and said received cryptographic authentication code match, then:

using said preliminary VLAN classification as a value of a VLAN classification parameter of any corresponding data request primitives;

decrypting said received frame using said table of security associations, and

submitting said decrypted frame to a forwarding and learning process;

wherein if said re-computed cryptographic authentication code and said received cryptographic authentication code do not match, then discarding said received frame.

39. (Previously presented): The method of claim 38 wherein said authentication code is a cryptographic authentication code which uniquely identifies a VLAN to which traffic belongs.

40. (Previously presented): The method of claim 38 wherein said authentication code key is generated during said initial authentication.

41. (Previously presented): The method of claim 38 wherein said initial authentication operation is performed between said end station and said access point.

42. (Currently amended): The method of claim 41 wherein said cryptographic message digest ~~method~~ algorithm is agreed upon by both said access point and said end station.